UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

PAXFIRE, INC.,	)	
	)	
Plaintiff,	)	
	)	
v.	)	**CASE NO.**
	)	
KIM RICHMAN,	)	
MILBERG LLP,	)	
MILBERG TADLER PHILLIPS	)	
GROSSMAN LLP,	)	
REESE RICHMAN, LLP,	)	
THE RICHMAN LAW GROUP	)	
REESE, LLP, and	)	
BETSY FEIST,	)	
	)	
Defendants.	)	

COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff PAXFIRE, INC. ("Paxfire"), by its undersigned attorneys, brings this action against the Defendants for malicious prosecution, that is, for the filing and pursuit of a meritless class action lawsuit against Paxfire, doing so with malice, for the purpose of damaging and destroying Paxfire and its business model. As a result of the lawsuit, Paxfire lost customers; lost a business opportunity to sell itself to a competitor; was forced to declare bankruptcy; and was forced out of business.

Paxfire seeks compensatory and punitive damages in an amount in excess of thirty million dollars ($30,000,000) in compensatory damages for special injuries; and fifty million dollars ($50,000,000) in punitive damages.

In furtherance of this Complaint, Paxfire states the following:

PARTIES AND CONSPIRATORS

A. Plaintiff Paxfire

1.   Plaintiff Paxfire, Inc. ("Paxfire") is a Delaware corporation, with its principal place of business in Northern Virginia, in the Commonwealth of Virginia. Paxfire's primary business was the provision of technology, that is, services based upon hardware and software devices, to Internet Service Providers ("ISPs"). Paxfire has no place of business in the State of New York.

B. The Defendants

2.   Defendant Betsy Feist ("Ms. Feist") resides in New York County, in the Southern District of New York, in the State of New York.

3.   Defendant Kim Richman ("Attorney Richman") is an attorney with the Richman Law Group, located at 81 Prospect Street, in Brooklyn, in the Eastern District of New York, in the State of New York.

4.   Defendant Reese Richman LLP ("Reese Richman") is a law firm with its offices located at 875 Avenue of the Americas, New York County, in the Southern District of New York, in the State of New York.

5.   Defendant Richman Law Group ("RLG") is a law practice located at 81 Prospect Street, Brooklyn, in the Eastern District of New York, in the State of New York.   It is a successor firm to the Defendant Reese Richman LLP, and regularly conducts business and derives revenue from New York County.

6.   Defendant Reese, LLP ("R-LLP") is a law firm located at 100 West 93rd Street, in the Southern District of New York, in the State of New York. It is a successor firm to the Defendant Reese Richman LLP.

7.   Defendant Milberg LLP ("Milberg") is a law firm with its principal offices located at One Pennsylvania Plaza, in the Southern District of New York, in the State of New York.

8.   Defendant Milberg Tadler Phillips Grossman LLP ("Milberg Tadler") is a law firm with its principal offices located at One Pennsylvania Plaza, in the Southern District of New York, in the State of New York. It is a successor firm to the Defendant Milberg.

C. Conspirators

9.   At all times pertinent to this Complaint, Conspirator the Electronic Frontier Foundation ("EFF") was and is an organization based in San Francisco, California, primarily involved in investigating, lobbying, and publicizing issues involving electronic privacy and civil liberties.

10.   At all times pertinent to this Complaint, the International Computer Science Institute ("ICSI") was and is an organization based in Berkeley, California, whose self-styled mission is listed on its website as: "Furthering computer science research through international collaboration. Furthering international collaboration through computer science research."

JURISDICTION AND VENUE

11.   This Court has jurisdiction over this Complaint pursuant to 28 U.S.C. § 1332(1), as the parties are citizens of different states and the amount in controversy is in excess of seventy-five thousand dollars ($75,000).

12.   This Court has personal jurisdiction over the Defendants as the Defendants filed the underlying lawsuit, *Feist v. RCN Corporation and Paxfire, Inc.*, Case No. 11-cv-5436 ("the

Underlying Action" or the "Feist Law Suit"), in the United States District Court for the Southern District of New York.

13.   Venue is appropriate in this District pursuant to 28 U.S.C. § 1391, as: (a) the underlying lawsuit that was the malicious prosecution alleged in this Complaint was filed in this District; and (b) several of the Defendants reside in this District and all Defendants reside in New York State.

PAXFIRE'S BUSINESS

A. Paxfire's Lines of Service

14.   At all times pertinent to the Underlying Action, Paxfire was involved in providing two lines of service to those Internet Service Providers ("ISPs") that contracted with Paxfire for such services, as part of the ordinary course of their own businesses for the provision of services to their customers. These lines of service were:

(a) **Error Redirection**, this being the provision of a webpage listing suggested website locations to Internet users who had typed invalid or otherwise unreachable web addresses into the address bars embedded in their web browsers; and

(b) **Direct Navigation**, this being the business of displaying and providing access to the websites of certain trademark holders to Internet users who entered these trademarks, or common misspelling of these trademarks (collectively, "Identified Trademarks"), into the address bars or search bars embedded in their web browsers.

15.   Paxfire generated income from Error Redirection: (a) by means of advertising that appeared on the webpages presented to users; (b) from "click through" traffic, when a user clicked on a link displayed in the user's web browser leading to an advertiser's website; and (c) when a user purchased a product or service after clicking on such a link.

16.   Paxfire generated income from Direct Navigation when a user purchased a product or service from a trademark holder whose website Paxfire presented in the user's web browser.

17.   At all times pertinent to the Underlying Action, Paxfire held contracts and had ongoing business relationships to provide Error Traffic services or Direct Navigation services, or both, with the following ISPs, among others: RCN Corporation, Cavalier, Cincinnati Bell, Cogent Communications, Frontier Communications, Insight Broadband, Iowa Telecom, DirectPC (Hughes Network), XO Communications, and Wide Open West.

18.   Paxfire shared with these ISPs the revenue that it generated from its services.

B. Paxfire's Technology

19.   As part of its method of business operations, Paxfire utilized a specialized computer, known as a "server," located physically inside of the network of an ISP and integrated into the ISP's network. This server was referred to as a Paxfire Lookup Engine, or "PLE."

20.   Electronic signals (excepting email) that a user generated by entering names, letters, or other characters, into the address bar of his or her web browser were transmitted by the user's ISP to Paxfire's PLE, within the ISP's network. These signals so transmitted by the ISP, and received by Paxfire, did not include signals generated by entries into the search box of a search engine's webpage (such as the webpage for Google, Bing, or Yahoo!); nor did it include email.

21.   The above described transmission of electronic signals by an ISP, and reception of such signals by Paxfire's PLEs, was done in the ordinary course of the ISP's business.

1. Error Redirection Technology

22.   When a Paxfire PLE detected an error in the entry typed by a user into the address bar of his or her web browser, the PLE transmitted a request to another specialized Paxfire server, known as a "proxy server." Based upon this this request, Paxfire's proxy server constructed a webpage containing suggestions for the user's consideration as to what the user may have intended to type into the address bar. It also included advertising in this constructed webpage. Paxfire then returned this webpage to the user's browser.

23.   At no time during the execution of Paxfire's Error Redirection technology did Paxfire disclose any electronic signal generated by the user to any third party.

2. Trademark Navigation

24.   When a Paxfire PLE detected an Identified Trademark, typed by a user into the address bar or search bar of his or her web browser, it transmitted this observation to the Paxfire proxy server. The proxy server then constructed a "link," or a special line of code (hereinafter the "Constructed Link") and transmitted this link to the website of the holder of the Identified Trademark, with a request that such website send its own webpage to the user's web browser.

25.   The Constructed Link did not contain electronic signals generated by the user. Instead, the link comprised two items: (i) the user's Internet Protocol ("IP") address, so that the trademark holder's website knew where to send its webpage; and (ii) a Publisher's ID number, informing the company that the visitor who made the purchase was sent to the trademark holder's website by the efforts of Paxfire. In this way Paxfire could receive a commission, and Paxfire and the user's ISP could receive a share of any revenue generated.

C. Paxfire's Privacy Policies

26.   At no time did Paxfire, know, identify, or record persons who were Internet users.

27.   At no time did Paxfire collect or compile information about Internet users in any manner that constituted profiling of such users or of the searches of such users.

28.   At no time did Paxfire share information about Internet users, or of their searches, with third parties.

29.   At no time did Paxfire sell information about Internet users or their searches.

30.   At no time did Paxfire allow third parties to access information about Internet users.

31.   At no time did Paxfire allow third parties to access searches by Internet users.

32.   At no time did Paxfire allow third parties to monitor searches by Internet users.

33.   At no time did Paxfire allow third parties to intercept searches by Internet users.

34.   At no time did Paxfire disclose confidential or private information relating to the use of the Internet by Internet users.

35.   At no time did Paxfire convert personal information of Internet users, including search histories, by providing such to third parties.

36.   At no time did Paxfire receive or retain money from third parties as a result of sharing or allowing access to the personal information of Internet users.

37.   At all times pertinent to the Underlying Action, Paxfire protected any and all information generated through the use of its services by Internet users.

THE CONSPIRACY

A. Improper Motives and the Manner and Means

38.   At all times pertinent to the Underlying Action, Defendants Ms. Feist, Attorney Richman, RLG, Reese-LLP, Reese Richman, and Milberg, together with EFF and the ICSI, collectively and individually, knew that Paxfire provided Error Redirection and Direct Navigation services to various ISPs, including the RCN Corporation ("RCN").

39.   At all times pertinent to the Underlying Action, the Defendants, EFF, and the ICSI opposed Paxfire's business practices of providing Error Traffic and Direct Navigation services to ISPs and Internet users. Quoting Peter Eckersley, the Technology Projects Director for EFF, EFF considered Paxfire's business practices to be "troubling," and "a deep violation of users' trust and expectations on how the Internet is supposed to function."

40.   The Defendants, EFF, and the ICSI opposed Paxfire's aforesaid business practices for the following reasons, among others:

(a) they wanted the Internet to function without recourse to services and technology implemented by Paxfire; and

(b) they wanted to stop, prevent, and deter "man in the middle" involvement in Internet traffic, regardless of whether such conduct was or was not lawful.

41.   In furtherance of the aforesaid purpose, the Defendants, EFF, and the ICSI agreed to act as vigilantes, that is, as self-appointed enforcement officials policing the Internet to deter conduct to which they objected.

42.   Among the Manner and Means whereby EFF and the ICSI carried out the aforesaid agreement were the following:

(a) assume the worst-case scenarios concerning the conduct in which Paxfire might be involved;

8

(b) intentionally avoid making any attempt to verify whether or not such worst-case conduct was actually occurring before taking overt action;

(c) bringing a class action lawsuit against Paxfire and one of Paxfire's contractual customers, this being RCN, alleging the aforesaid unverified, false allegations of worst-case conduct;

(d) publishing the false worst-case allegations on websites, blogs, and other electronic media, doing so in support of their class action complaint; and

(e) "blindsiding" Paxfire with regard to this class action lawsuit.

43.   By the aforesaid manner and means, the Defendants, EFF and the ICSI destroyed Paxfire and forced Paxfire into bankruptcy.

B. Pre-Suit Overt Acts

44.   In furtherance of and to effect the purposes of this conspiracy, on or about July 24, 2011, Attorney Richman solicited Defendant Feist to bring a class action lawsuit against Paxfire.

45.   In furtherance of and to effect the purposes of this conspiracy, on or about July 26, 2011, Defendant Feist agreed to file such class action lawsuit against Paxfire.

46.   In furtherance of and to effect the purposes of this conspiracy, the Defendants, EFF, and the ICSI engaged in the following conduct:

(a) On or about August 1, 2011, Christian Kreibich of the ICSI sent an email to the attorneys for Ms. Feist, including Attorney Richman and lawyers with Milberg and Reese Richman, and to Jim Giles of the New Scientist, a media outlet on the Internet (Exhibit 1). This email reads in pertinent part:

> Allow me to introduce you to Jim Giles, the reporter at New Scientist who's currently working on a story on the Paxfire affair. Jim, meet the legal front! Jim

9

has been investigating Paxfire's search redirections for quite some time now and is fully up to date on our findings, so it seems helpful for all of you to have each other's contact information.

(b) Sometime during the period August 1 to noon on August 4, 2011, Eastern Time, Ms. Feist's attorneys, these being Defendants Milberg, Reese Richman, and Attorney Richman (collectively, Ms. Feist's "Defendant Attorneys"), communicated with Jim Giles of the New Scientist (Exhibit 2), informing him that Defendant Feist would file a Class Action Complaint on August 4, 2011, and making numerous false and defamatory statements about Paxfire. These statements were made to the New Scientist for the purpose of causing an article with these statements to be published and republished on the Internet and elsewhere. Among these false and defamatory statements were the following:

   (i)   that Paxfire "hijacked" searches of millions of Internet users;

   (ii)   that Paxfire violated numerous statutes, including wiretapping laws; and

   (ii)   that Paxfire violated "privacy safeguards enshrined" in the 1968 Wiretap

Act.

(c) On August 4, 2011, in preparation for her filing a class action lawsuit against Paxfire, Ms. Feist, through her Defendant Attorneys, induced and otherwise caused the New Scientist to publish an article on the Internet falsely stating that Paxfire's business practices violated numerous statutes, including wiretapping laws;

(d) On August 4, EFF and ICSI published on the EFF website and blog an article alleging, among other false and misleading representations:

   (i) That Paxfire's proxies collected a user's web searches and the corresponding web search results; whereas in truth and in fact, Paxfire's proxies only logged a small subset of search queries that were entered into a browser search box, related to certain

10

trademark holders with whom Paxfire had a direct or indirect business contract or relationship, doing so anonymously, without identifying individual Internet users; and

(ii) That Paxfire's practices allowed Paxfire and/or its ISP customers to directly monitor all searches made by Internet users and to build up corresponding profiles; whereas, in truth and fact, while Paxfire's code examined queries and responses, it selected out and logged only those that were of relevance to its business for accounting and debugging purposes, maintained the confidentiality of such logs from any and all third parties, and did so anonymously, without identifying individual users.

C. The Underlying Action: Ms. Feist's Class Action Lawsuit

47. On August 4, 2011 Defendant Feist and her Defendant Attorneys filed the Underlying Action, a class action lawsuit, in the Southern District of New York, naming Paxfire and RCN as defendants.

48. Defendant Feist and her Defendant attorneys made false, misleading, and defamatory statements and representations in her Underlying Action, including that:

a) Paxfire identified persons who were Internet users and engaged in searches using the Internet;

b) Paxfire collected and compiled information about Internet users in a manner that constituted profiling of such Internet users, or of the searches of such End Users;

c) Paxfire shared information about Internet users, or of their searches, with third parties;

d) Paxfire sold information about Internet users or of their searches;

e) Paxfire allowed third parties to access information about Internet users;

f)   Paxfire allowed third parties to access searches by Internet users;

g)   Paxfire allowed third parties to monitor searches by Internet users;

h)   Paxfire allowed third parties to intercept searches by Internet users;

i)   Paxfire disclosed confidential or private information relating to the use of the Internet by Internet users;

j)   Paxfire converted personal information of Internet users, including search histories, by providing such to third parties;

k)   Paxfire received or retained money from third parties as a result of sharing and/or allowing access to the personal information of Internet users; and

l)   Paxfire engaged in violation of wiretap statutes affecting Internet users.

49.   At the time that Defendant Feist and her Defendant Attorneys made these allegations in her class action lawsuit, they knew that these allegations were false, and knew that they did not have evidence as to the truth of such statements.

50.   The class action lawsuit that comprised the Underlying Action was frivolous, and the Defendant Feist and her Defendant Attorneys then well knew so.

D. The Malicious Conduct of the Defendants

1. Deliberately Ignoring the Authorization in RCN's Privacy Policy

51.   Defendant Feist and her Defendant Attorneys conceded in the Underlying Action that RCN had a Privacy Policy, and that this policy was applicable to her use of RCN's services. This concession appeared in Paragraphs 29 through 30 of her class action Complaint.

52.   The second paragraph of RCN's Privacy Policy reads:

> As a customer of RCN, you are agreeing to the terms of this Privacy Policy, and revisions made to the Privacy Policy from time to time (see VI. Revision of This Policy), unless and until you terminate your RCN services.

12

53.   In her class action Complaint, Ms. Feist and her Defendant Attorneys quoted a portion of the Privacy Policy of RCN for the purpose of bolstering her claims. Specifically, she quoted the following paragraph in Paragraph 28 of her Compliant:

> At RCN, the privacy and security of your account is very important to us. That is why we have taken measures to protect the privacy of your personally identifiable account records and to comply with the federal laws and FCC regulations that govern use and disclosure of customer information.

54. Despite reading, relying upon, and quoting this portion of her agreement with RCN in her class action Complaint, Ms. Feist and her Defendant Attorneys **deliberately ignored** that part of the RCN Privacy Policy whereby Ms. Feist **authorized** RCN, and Paxfire acting as RCN's agent, to do exactly what Ms. Feist and her attorneys alleged that RCN, and Paxfire did in violation of law. For example and specifically, Part I.A of RCN's Privacy Policy provided (bold added):

> Non-Personally Identifiable Information and Aggregated Data collected via RCN's network, as described in Section II.D above, is used by RCN and **third parties**:
>
> • to understand how the RCN network is operating and being used
> • to monitor quality of service
> • to analyze aggregate customer behavior to assist RCN in improving and marketing its services
> • for RCN marketing, sales, and consumer retention efforts
> • **for third party marketing and advertising purposes**
>
> RCN may use Personally Identifiable Information or CPNI, collected via RCN's network, as described in Section II.D above:
> • to measure subscriber satisfaction
> • to improve services and marketing
> • **to establish individual customer profiles for targeted advertising and customer retention purposes**

55.   The action of Defendant Feist and her Defendant Attorneys in deliberately ignoring the above portion of the RCN privacy Policy, while quoting other portions of the policy,

demonstrated that they aware that the claims in the Underlying Action were frivolous and establishes that they acted with malice against Paxfire.

2. Misrepresentation of the Netalyzr

56.   On or about July 24, 2011, Ms. Feist and Attorney Richman, working together by telephone, used a software application known as the "Netalyzr," provided by ICSI, to supposedly examine Paxfire's services.

57.   In the class action Complaint that they filed in the Underlying Action, Defendant Feist and her Defendant Attorneys alleged that that the Netalyzr demonstrated the following:

(a) that Paxfire collected the personal search histories of individual Internet users,

(b) that Paxfire profiled such users by their search histories; and

(c) that Paxfire sold these search histories and otherwise disclosed these histories.

58.   These allegations were false, in that Paxfire did not do or engage in the above cited actions and conduct.

59.   In fact, the Netalyzr did not have the ability to determine, and could not determine, whether or not Paxfire engaged in the above described actions and conduct: while the Netalyzr was capable of determining to a limited extent **the routing** of electronic signals transmitted on the Internet, it had **no ability** to determine what anyone involved in those transmission **was doing** with any of the information transmitted.

60.   The action of Defendant Feist and her Defendant Attorneys in fabricating the capabilities and findings of the Netalyzr demonstrated that they aware that the claims in the Underlying Action were frivolous and establishes that they acted with malice against Paxfire.

3. The Defendants Purposely Avoiding Making Inquiries to Paxfire

61.   Prior to filing the class action Complaint in the Underlying Action, Defendant Feist and her Defendant Attorneys communicated with NEW SCIENTIST for the purpose of publicizing their Complaint and the allegations and claims in their Complaint.

62.   Prior to filing the class action Complaint in the Underlying Action, the Defendant Feist and her Defendant Attorneys avoided contacting Paxfire, or making any attempt to contact Paxfire, so as to determine whether the allegations and claims that they made in their Complaint were factually accurate.

63.   The action of Defendant Feist and her Defendant Attorneys in avoiding any contact with Paxfire was deliberate, as demonstrated by their purposeful contact and communication with NEW SCIENTIST.

64.   The deliberate action of Defendant Feist and her Defendant Attorneys in avoiding any contact with Paxfire to determine whether the allegations and claims that they made in their Complaint were factually accurate demonstrates that they were aware that their allegations and claims were frivolous, and establishes that they acted with malice against Paxfire.

E. Further Bad Faith on the Part of Defendant Feist and Her Conspirators

1. Feist Destroyed Evidence

65.   After filing the class action Complaint in the Underlying Action, Defendant Feist ran a software program on her personal computer, this being Piroform's CCleaner ("CCleaner"). One effect of running this program was the erasure of all evidence that could establish or disprove whether Paxfire had intercepted or otherwise acquired any Identified Trademark that Ms. Feist may have entered into the search bar of her web browser.

15

66.   Defendant Feist's destruction of the evidence of her interactions with Paxfire, if any occurred, after the filing of her class action Complaint, and the failure of her Defendant Attorneys to take action to protect such evidence, demonstrated their bad faith in pursuing her Underlying Action.

67.   The Court in the Underlying Action sanctioned Defendant Feist for this conduct (Doc. No. 249), ruling that:

> Because Paxfire cannot access Feist's cookies to determine which redirections are attributable to Paxfire's conduct, the Court precludes Feist from arguing that statutory damages are to be awarded in this case for specific redirections, and specific internet searches. Feist may not proffer any evidence of specific violations in its motion for summary judgment, or at trial.

2. ICIS Took Money from Feist's Attorneys, Failing to Disclose This Fact

68.   On or about the period August 31 through September 2, 2011, Vernon Paxson, Christian Kreibich, and Nicholas Weaver of ICSI, executed an agreement with Feist's Defendant Attorneys whereby they would each receive a bounty, in the amount of $300 per hour, for uncovering additional entities involved in "redirecting and/or proxying searches"; and for assisting Defendant Feist and her Attorneys in the Underlying Action.

69.   While presenting themselves on the EFF website and blog as neutral third parties, and while characterizing their actions in publicizing Paxfire's conduct as taken solely for research purposes and for the public good, Vernon Paxson, Christian Kreibich, and Nicholas Weaver failed to disclose and otherwise withheld from the public the fact that they had a financial interest in the civil prosecution of Paxfire.

3. EFF Misled the Federal Courts

70.   In an effort to impede and obstruct Paxfire's defense in the Underlying Action, Peter Eckersley of EFF executed two separate declarations, submitting the first in the United

States District Court for the Southern District of New York in or about September, 2011; and submitting the second in the United States District Court for the Northern District of California, in or about June, 2012. These declarations **contradicted each other in a material matter**—this being whether or not Mr. Eckersley was an expert consultant for Defendant Feist.

71.   In his first affidavit, in the Southern District of New York, submitted in the Underlying Action by Feist's Defendant Attorneys, Mr. Eckersley declared under penalty of perjury as follows (emphasis added): "**I am not a consultant or expert for plaintiff in this case**, and I have not received and will not receive compensation for providing this declaration," asserting thereby that he was neither a consultant or expert for Ms. Feist, nor was being paid by Ms. Feist for providing his declaration.

72.   In his second declaration, in the Northern District of California, made in an effort to avoid complying with subpoenas served upon him and EFF by Paxfire in the Underlying Action, Mr. Eckersley declared under penalty of perjury that he *was* an expert and consultant for Defendant Feist as follows (emphasis added):

> At some point during these conversations, it was decided that I would not act as a paid expert consultant in this particular matter. As a result, neither EFF nor I were retained as paid consultants by Plaintiff's counsel. **However, Plaintiff's counsel consulted me and EFF in our capacity as experts in the technology at issue, industry practices, and related law and policy.**

73.   Mr. Eckersley filed his second declaration in the Northern District of California for the purpose of relying upon the evidentiary protections afforded to experts and consultants, to prevent Paxfire from obtaining his testimony and certain documents in the possession of EFF.

\

17

THE CLASS ACTION COMPLAINT AND
ITS ULTIMATE TERMINATION IN FAVOR OF PAXFIRE

74.   On August 4, 2011. Defendant Feist and her Defendant Attorneys, specifically,

Attorney Kim Richman as well as the law firms Milberg, LLP and Reese Richman, LLP, filed a

class action Complaint in the Underlying Action naming both Paxfire and RCN as defendants.

75.   Defendant Feist and her Defendant Attorneys named Paxfire as a defendant in

three counts in their class action Complaint.   These counts were:

Count	Claim	Legal Basis
I	Electronic Communications Protections Act (ECPA)	18 U.S.C. § 2510
IV	Conversion	N.Y. Common Law
V	Unjust Enrichment	N.Y. Common Law

76.   Paxfire filed counterclaims, including defamation claims for slander and libel,

against Ms. Feist.

77.   On December 14, 2012, Paxfire filed for bankruptcy in the United States

Bankruptcy Court for the Eastern District of Virginia, No. 12-17341.

78.   Defendant Feist and her Defendant Attorneys purposely avoided filing any proof

of claim, on behalf of Ms. Feist or on behalf of the class that she purportedly represented.

79.   On December 17, 2015, Paxfire filed its motion in the Underlying Action

captioned, "Defendant Paxfire's Motion to Restrict Recovery of Plaintiff Betsey Feist to Setoff

of Paxfire's Counterclaims, and to Disqualify Feist as Lead Plaintiff in Any Class Action," (Doc.

No. 178 (the "Motion"). By Letter filed in the Underlying Action dated January 19, 2016 (Doc.

No. 188), Paxfire and Defendant Feist, through her attorneys Defendants Milberg, Kim Richman,

and RLG, stipulated to the remedies sought in the Motion.

80. By Order dated January 22, 2016, (Doc. No. 191) the Court in the Underlying Action granted Paxfire's Motion as follows:

> Having received the Parties' stipulation regarding Defendant Paxfire's motion to restrict recovery of Feist to setoff of Paxfire's counterclaims, and to disqualify Feist as Lead Plaintiff (Doc. No. 188-1),
>
> **IT IS HEREBY ORDERED** that any recovery to which Feist may be entitled is limited to setoff of her personal claims against Paxfire's counterclaims.

81. By Order (Doc. No. 253) dated January 17, 2017, the Court in the Underlying Action dismissed the remainder of Defendant Feist's Complaint, holding (emphasis added):

> For the foregoing reasons, Feist's motion for summary judgment on Paxfire's counterclaims is GRANTED. **Feist's claims are DISMISSED as moot in light of her stipulation to limit recovery on her claims to the amount necessary to offset Paxfire's recovery on its counterclaims.** Consequently, Paxfire's motion for summary judgment on Feist's claims is DENIED as moot.

82. Feist took nothing from Paxfire as a result of her class action Complaint and the Underlying Action. Based upon this, and based upon the orders of the Court in the Underlying Actions sanctioning Ms. Feist (Doc. 249); disqualifying Ms. Feist as lead plaintiff in her class action (Doc. 191); restricting the recovery to which Ms. Feist's might have been entitled to only the setoff of her personal claims (Doc 191); and dismissing her personal claims (Doc. 253)—the Underlying Action terminated favorably for Paxfire.

THE LACK OF PROBABLE CAUSE

83. Prior to filing their class action Complaint in the Underlying Action, Defendant Feist and her Defendant Attorneys knew that they did not have probable cause for any of the claims that they asserted in their class action Complaint.

84. The Defendants knew that Paxfire had a contractual and business relationship with RCN and other ISPs, and that the transmission, the reception, and the consequential

19

interception of electronic signals by such ISPs and Paxfire fell within the "Ordinary Course of Business" safe harbor provision in the Electronic Communications Protections Act ("ECPA"), 18 U.S.C. § 2510(5)(a)(ii).

85.   To the extent that Count One of their class action Complaint asserted a claim for the interception of electronic signals and communications, the Defendants knew that this claim was frivolous due to the aforesaid safe harbor provision of ECPA.

86.   The Defendants knew that Paxfire routed electronic signals of Internet users to its own proxy servers, and such routing did not comprise a disclosure to any third party not under contract to itself.

87.   To the extent that Count One of their class action Complaint asserted a claim for the disclosure of electronic signals and communications to third parties, the Defendants knew that this claim was frivolous due to the aforesaid routing of electronic signals to itself and not to third parties.

88.   Defendant Feist never had standing to bring either personal claims or class action claims for Direct Navigation, as she confirmed in her deposition testimony that she did not enter into the search bar of her web browser any Identified Trademarks, or at best could not remember entering any Identified Trademarks into her web browser; and as a result, she could not assert any claims under Counts One, Four, and Five.

89.   To the extent that Counts One, Four and Five of their class action Complaint asserted claims for the interception, collection, and profiling, of electronic signals, communications, and searches, and for the disclosure and sale of such information to third parties, the Defendants knew that this claim was frivolous due to the inability of Defendant Feist to establish that Paxfire intercepted any of the entries she may have made in the search bar of her web browser.

20

90.   Defendant Feist agreed to Part I.A of RCN's Privacy Policy, which permitted

RCN to disclose her personal identifying and non-identifying information for the purpose of

advertising.

91.   Defendant agreed to Part II.D of RCN's Privacy Policy, which further permitted

RCN to disclose her personal identifying and non-identifying information for multiple [purposes,

including advertising, explaining as follows (emphasis added):

> RCN's servers, **and servers connected to the RCN network by authorized
> third parties for data collection purposes, also collect certain information**. As
> is common practice in our industry, RCN may use web caching software on its
> network to ensure optimum performance for our customers. Such software by its
> nature captures Internet Protocol and URL information to a log file. The RCN
> network also automatically logs certain information, such as application usage
> and type. Such logs generally are maintained on RCN's secured servers and/or the
> secured servers of authorized third parties as long as is necessary to fulfill a
> legitimate business or law enforcement need. Typically, information collected by
> servers connected to the RCN network is maintained as NonPersonally
> Identifiable Information and/or Aggregated Data. **However, this information
> may become Personally Identifiable Information if and when RCN associates
> the information with a particular customer's account for marketing,**
> customer retention, or network security and reliability purposes. This data may
> also be used to protect the security of RCN's network, to prevent network
> intrusions from viruses and worms, and for advertising purposes. **Specifically,
> RCN and certain third parties authorized by RCN have the ability to
> monitor all network traffic destined to and from any connected device
> attached to RCN's network. However, authorized third parties, which may
> collect this information for marketing,** customer retention, product
> development, or advertising purposes, do not receive any Personally Identifiable
> Information from RCN regarding RCN's customers, but rather collect the data on
> an anonymous and/or aggregated basis. In most cases, network traffic monitoring
> is restricted to viewing source/destination addresses, and the content of the
> transaction is not viewed. **However, the information collected may include
> URLs of web sites you have visited** and the content of any unencrypted email or
> other communications sent by or to you . . . .

92.   To the extent that Counts One, Four and Five of their class action Complaint

asserted claims for the interception, collection, and profiling, of electronic signals,

communications, and searches, and for the disclosure and sale of such information to third

parties, the Defendants knew that this claim was frivolous due to express terms of Parts I.A and II.D of the RCN Policy Agreement to which Ms. Feist agreed and terms of which she relied upon in her class action Complaint.

SPECIAL DAMAGES

93.   At all times pertinent to these the Underlying Action Paxfire had a contract and an ongoing business relationship with each the RCN Corporation and other ISPs, including Cavalier, Cincinnati Bell, Cogent Communications, Frontier Communications, Insight Broadband, Iowa Telecom, DirectPC (Hughes Network), XO Communications, Wide Open West; Global Crossing, Sprint, LocalNet, Earthlink, and Verizon Business.

94.   At all times pertinent to this Complaint, Paxfire was in negotiations with Xerocole, Inc., an Internet company, for the sale of Paxfire to such company; and such company intended to make an offer during the week of August 11, 2011, of at least $10 million plus additional monetary considerations, for Paxfire's assets or equity, or for both.

95.   At all times pertinent to this Complaint, Paxfire was in negotiations with AdKnowledge, Inc., an Internet company, for the sale of Paxfire to such company; and such company intended to make a monetary offer for Paxfire's assets or equity, or for both.

96.   During 2009, a foreign Internet company had made an offer for the purchase of Paxfire, and its assets or equity, or both, valuing such at forty-million dollars.

97.   By and through the scheme described above, executed in concert by the coconspirators Defendant Feist, Feist's Defendant Attorneys, EFF, and the ICSI, intentionally disparaged and damaged Paxfire by filing the class action lawsuit in the Underlying Action; publishing the above described article on the EFF website and blog; presenting the above described paper disparaging Paxfire; and publishing to the New Scientist the above described

22

false statements for the purpose of causing NEW SCIENTIST to publish such statements in an article on the Internet, which NEW SCIENTIST did on August 4, 2011.

COUNT ONE

98.   Plaintiff Paxfire realleges and reincorporates by reference the allegations contained in paragraphs one through ninety-seven of these counterclaims and further alleges:

99.   On August 4, 2011, the Defendants, Kim Richman, Reese Richman, LLP, Milberg, LLP, and Betsey Feist, filed a class action lawsuit (the "Feist Class Action") against the Plaintiff Paxfire, Inc., intentionally doing so without probable cause for the causes of action contained therein.

100.   Beginning on August 4, 2011 and continuing until January 17, 2017, the aforesaid defendants pursued and litigated the Feist Class Action, doing so in the Underlying Action, by and on at the instance of Betsy Feist both as an individual plaintiff and as lead plaintiff on behalf of the classes identified therein.

101.   During the period on or about August 1, 2011 and continuing until an unknown date, pursuant and ancillary to, and in support of the Underlying Action, the Defendants and their conspirators published and caused to be published articles about Paxfire that included the false and disparaging allegations contained in the Feist Class Action.

102.   At all times pertinent to the Underlying Action, the Defendants, Kim Richman, Reese Richman, LLP, Milberg, LLP, and Betsey Feist, intentionally filed, pursued, and litigated the Feist Class Action with malice, for a purpose other than for any violation of statutory or common law.

103.   On January 17, 2017, the Underlying Action terminated favorably for Paxfire, defendant in the Underlying Action and plaintiff in this Complaint.

104.   As a result of the aforesaid malicious prosecution by the Defendants, Kim Richman, Reese Richman, LLP, Milberg, LLP, and Betsey Feist, Paxfire suffered special damages.

105.   In their capacities as successor entities of Defendant Reese Richman, LLP, the Defendant Richman Law Group and the Defendant Reese, LLP are liable to the same extent, individually and severally, as is Reese Richman, LLP.

106.   In its capacity as the successor entity of Defendant Milberg, LLP, the Defendant Milberg Tadler Phillips Grossman LLP is liable to the same extent as is Milberg, LLP.

REQUEST FOR RELIEF

Plaintiff Paxfire, Inc. asks for judgment in its favor as follows:

1.   Judgment be entered against the Defendants, jointly and severally, in favor of Paxfire in the amount of thirty million dollars ($30,000,000) for special damages and fifty million dollars ($50,000,000) in punitive damages;

2.   Paxfire be awarded attorneys' fees costs, and expenses; and

3.   Such other and further relief as the Court deems just and proper.

JURY TRIAL DEMAND

Plaintiff Paxfire requests trial by jury of all claims that may be tried in the United States

District Court for the Southern District of New York.

Respectfully Submitted,

/s/Andrew Grosso

Andrew Grosso, Esq.
(N.Y. State Bar No. 1723337)
ANDREW GROSSO & ASSOCIATES
Georgetown Place
1101 Thirtieth Street, NW, Suite 300
Washington, 20007
(202) 298-6500 Tel.
Agrosso@acm.org Email

OF COUNSEL:

Stephen J. Bagge
(Florida Bar No. 97788)
STEPHEN J. BAGGE, P.A.
3902 Henderson Blvd. Suite 208-30
Tampa, Florida 33629
(813) 250-0511 Tel.
sbagge@baggelaw.com Email

Ronald J. Jarvis
(D.C. Bar No. 292243)
ANDREW GROSSO & ASSOCIATES
Georgetown Place
1101 Thirtieth Street, NW, Suite 300
Washington, 20007
(202) 298-6500 Tel.
RJJarvis@gmail.com Email

James Moody
(D.C. Bar No. 294504)
ANDREW GROSSO & ASSOCIATES
Georgetown Place
1101 Thirtieth Street, NW, Suite 300
Washington, 20007
(202) 298-6500 Tel.
MoodyJim@aol.com Email

Arnon D Siegel
(N.Y. State Bar No. No. 446770)
655 Avenue of the Americas, No. 3-D
New York, New York 10010
(202) 460-4236 Tel.
Arnon.Siegel@gmail.com Email

Dated: January 16, 2018